CLAIMS

What is claimed is:

1. In a server adapted for authentication, authorization, and accounting, a method of generating a shared key between a Home Agent and a Mobile Node, comprising:

receiving a request message from a Home Agent, the request message identifying the Mobile Node;

deriving key information from a key or password associated with the Mobile Node; and

sending a reply message to the Home Agent, the reply message including the key information associated with the Mobile Node, thereby enabling the Home Agent to derive a shared key to be shared between the Mobile Node and the Home Agent from the key information.

2. The method as recited in claim 1, wherein deriving key information comprises:

deriving the key information from a second set of key information derived from the key or password.

3. The method as recited in claim 1, wherein deriving key information comprises:

obtaining the derived key information from a domain controller or server.

4. The method as recited in claim 1, wherein the request message is an access request message and the reply message is an access reply message.

5. The method as recited in claim 1, wherein the key or password comprises a Windows password associated with the Mobile Node.

6. The method as recited in claim 5, further comprising:

obtaining the key or password from a domain controller.

7. The method as recited in claim 6, wherein obtaining the key or password from the domain controller comprises:

sending a request to the domain controller for key or password associated with the Mobile Node; and

receiving the key or password associated with the Mobile Node from the domain controller.

8. The method as recited in claim 1, further comprising:

applying the key information to authenticate the request message.

9. The method as recited in claim 1, wherein the key or password is stored at the Mobile Node, thereby enabling the Mobile Node to derive the key information from the key or password.

10. In a Home Agent supporting Mobile IP, a method of authenticating a Mobile Node, comprising:

receiving a registration request from a Mobile Node, the registration request identifying the Mobile Node;

sending a request message to a AAA server, the request message identifying the Mobile Node;

receiving a reply message from the AAA server, the reply message including key information associated with the Mobile Node;

deriving a key from the key information, the key being a shared key between the Mobile Node and the Home Agent; and

sending a registration reply to the Mobile Node.

11. The method as recited in claim 10, wherein the registration request includes a CHAP challenge and response.

12. The method as recited in claim 10, wherein deriving a key from the key information comprises deriving the key from the key information and a CHAP challenge and response obtained from the registration request.

13. The method as recited in claim 10, wherein deriving the key and sending the registration reply to the Mobile Node are performed when the reply message received from the AAA server indicates that the Mobile Node is successfully authenticated.

14. The method as recited in claim 10, wherein the request message is an access request message and the reply message is an access reply message.

15. The method as recited in claim 10, wherein the Mobile Node is to derive the shared key from a second set of key information stored at the Mobile Node.

16. The method as recited in claim 15, wherein the key information is equivalent to the second set of key information.

17. The method as recited in claim 15, wherein the second set of key information stored at the Mobile Node is a root key, a password, or a key shared between the Mobile Node and the Home Agent in a previous session.

18. The method as recited in claim 17, wherein the registration request includes a SPI, replay protection timestamp, and indicates an algorithm to be used to authenticate the registration reply, wherein the SPI, the replay protection timestamp, and the algorithm are associated with the second set of key information.

19. The method as recited in claim 18, further comprising:

installing the derived key, the SPI, the replay protection timestamp, and the algorithm in a security association.

20. The method as recited in claim 17, wherein the registration reply includes a SPI, replay protection timestamp, and indicates an algorithm to be used to authenticate the registration reply, wherein the SPI, the replay protection timestamp, and the algorithm are associated with the second set of key information.

21. The method as recited in claim 10, wherein the registration reply indicates that the Mobile Node is to derive the shared key between the Mobile Node and the Home Agent.

22. The method as recited in claim 21, wherein at least one of the presence of one or more extensions in the registration reply and an SPI in the registration reply indicates that the Mobile Node is to derive the shared key between the Mobile Node and the Home Agent.

23. The method as recited in claim 10, wherein the registration request indicates that the Home Agent is to derive the shared key between the Mobile Node and the Home Agent from the key information.

24. The method as recited in claim 23, wherein at least one of the presence of one or more extensions in the registration request and an SPI in the registration request indicates that the Home Agent is to derive the shared key between the Mobile Node and the Home Agent.

25. The method as recited in claim 23, wherein the presence of an authentication protocol extension in the registration request indicates a protocol to be used to authenticate the registration request and derive the shared key.

26. The method as recited in claim 23, wherein the presence of a session key extension and derived session key extension in the registration request indicates that both a session key and a derived session key are to be generated and installed.

27. The method as recited in claim 26, further comprising:

receiving a subsequent registration request from the Mobile Node to refresh the derived session key.

28. The method as recited in claim 27, further comprising:

authenticating the subsequent registration request using the session key.

29. The method as recited in claim 27, further comprising:

sending a subsequent registration reply to the Mobile Node including the derived session key extension, wherein the registration reply is to be authenticated by

the Mobile Node using the session key.

30. The method as recited in claim 10, wherein the key information is a previously used session key shared between the Mobile Node and the Home Agent.

31. The method as recited in claim 10, wherein the key information is derived from a password associated with the Mobile Node.

32. The method as recited in claim 31, wherein the password is a Windows password.

33. The method as recited in claim 10, further comprising:

deriving a subsequent key from the shared key.

34. The method as recited in claim 33, wherein deriving the subsequent key from the shared key is performed when a binding associated with the Mobile Node is cleared.

35. The method as recited in claim 34, wherein the binding associated with the Mobile Node is cleared upon expiration of the lifetime of the Mobile Node or de-registration of the Mobile Node.

36. In a Mobile Node, a method of registering with a Home Agent supporting Mobile IP, comprising:

sending a registration request to the Home Agent;

receiving a registration reply from the Home Agent, the registration reply indicating that the Mobile Node is to derive a key to be shared between the Mobile Node and the Home Agent; and

deriving a key to be shared between the Mobile Node and the Home Agent from key information stored at the Mobile Node.

37. The method as recited in claim 36, wherein deriving a key from the key information comprises deriving the key from the key information and a CHAP challenge and response obtained from the registration reply.

38. The method as recited in claim 36, wherein the key information is a root key, a password, or a key shared between the Mobile Node and the Home Agent in a previous session.

39. The method as recited in claim 38, wherein the registration request includes a SPI, replay protection timestamp, and indicates an algorithm to be used to authenticate the registration request, wherein the SPI, the replay protection timestamp, and the algorithm are associated with the key information.

40. The method as recited in claim 38, wherein the registration reply includes a SPI, replay protection timestamp, and indicates an algorithm to be used to authenticate the registration reply, wherein the SPI, the replay protection timestamp, and the algorithm are associated with the key information.

41. The method as recited in claim 36, wherein the registration reply indicates whether the Mobile Node is to derive the shared key between the Mobile Node and the Home Agent, the method further comprising:

determining from the registration reply whether the Mobile Node is to derive the key;

wherein deriving a key is performed when it is determined from the registration reply that the Mobile Node is to derive the key.

42. The method as recited in claim 41, wherein at least one of the presence of one or more extensions in the registration reply and an SPI in the registration reply

indicates that the Mobile Node is to derive the shared key between the Mobile Node and the Home Agent.

43. The method as recited in claim 36, wherein the registration request indicates that the Home Agent is to derive the shared key between the Mobile Node and the Home Agent from a second set of key information received by the Home Agent.

44. The method as recited in claim 43, wherein at least one of the presence of one or more extensions in the registration request and an SPI in the registration request indicates that the Home Agent is to derive the shared key between the Mobile Node and the Home Agent.

45. A computer-readable medium storing thereon computer readable instructions for generating a shared key between a Home Agent and a Mobile Node in a server adapted for authentication, authorization, and accounting, comprising:

instructions for receiving a request message from a Home Agent, the request message identifying the Mobile Node;

instructions for deriving key information from a key or password associated with the Mobile Node; and

instructions for sending a reply message to the Home Agent, the reply message including the key information associated with the Mobile Node, thereby enabling the Home Agent to derive a shared key to be shared between the Mobile Node and the Home Agent from the key information.

46. A server adapted for authentication, authorization, and accounting, the server being adapted for generating a shared key between a Home Agent and a Mobile Node, comprising:

a processor; and

a memory, at least one of the processor and the memory being adapted for:

receiving a request message from a Home Agent, the request message identifying the Mobile Node;

deriving key information from a key or password associated with the Mobile Node; and

sending a reply message to the Home Agent, the reply message including the key information associated with the Mobile Node, thereby enabling the Home Agent to derive a shared key to be shared between the Mobile Node and the Home Agent from the key information.

47. A server adapted for authentication, authorization, and accounting, the server being adapted for generating a shared key between a Home Agent and a Mobile Node, comprising:

means for receiving a request message from a Home Agent, the request message identifying the Mobile Node;

means for deriving key information from a key or password associated with the Mobile Node; and

means for sending a reply message to the Home Agent, the reply message including the key information associated with the Mobile Node, thereby enabling the Home Agent to derive a shared key to be shared between the Mobile Node and the Home Agent from the key information.

48. A computer-readable medium storing thereon computer-readable instructions for authenticating a Mobile Node in a Home Agent supporting Mobile IP, comprising:

instructions for receiving a registration request from a Mobile Node, the registration request identifying the Mobile Node;

instructions for sending a request message to a AAA server, the request message identifying the Mobile Node;

instructions for receiving a reply message from the AAA server, the reply message including key information associated with the Mobile Node;

instructions for deriving a key from the key information, the key being a shared key between the Mobile Node and the Home Agent; and

instructions for sending a registration reply to the Mobile Node.

49. A Home Agent supporting Mobile IP, the Home Agent being adapted for

authenticating a Mobile Node, comprising:

a processor; and

a memory, at least one of the processor and the memory being adapted for:

receiving a registration request from a Mobile Node, the registration request identifying the Mobile Node;

sending a request message to a AAA server, the request message identifying the Mobile Node;

receiving a reply message from the AAA server, the reply message including key information associated with the Mobile Node;

deriving a key from the key information, the key being a shared key between the Mobile Node and the Home Agent; and

sending a registration reply to the Mobile Node.

50. A Home Agent supporting Mobile IP and adapted for authenticating a Mobile Node, comprising:

means for receiving a registration request from a Mobile Node, the registration request identifying the Mobile Node;

means for sending a request message to a AAA server, the request message identifying the Mobile Node;

means for receiving a reply message from the AAA server, the reply message including key information associated with the Mobile Node;

means for deriving a key from the key information, the key being a shared key between the Mobile Node and the Home Agent; and

means for sending a registration reply to the Mobile Node.

51. A computer-readable medium storing thereon computer-readable instructions for registering a Mobile Node with a Home Agent supporting Mobile IP, comprising:

instructions for sending a registration request to the Home Agent;

instructions for receiving a registration reply from the Home Agent, the registration reply indicating that the Mobile Node is to derive a key to be shared between the Mobile Node and the Home Agent; and

instructions for deriving a key to be shared between the Mobile Node and the Home Agent from key information stored at the Mobile Node.

52. A Mobile Node adapted for registering with a Home Agent supporting Mobile IP, comprising:

a processor; and

a memory, at least one of the processor and the memory being adapted for:

sending a registration request to the Home Agent;

receiving a registration reply from the Home Agent, the registration reply indicating that the Mobile Node is to derive a key to be shared between the Mobile Node and the Home Agent; and

deriving a key to be shared between the Mobile Node and the Home Agent from key information stored at the Mobile Node.

53. A Mobile Node adapted for registering with a Home Agent supporting Mobile IP, comprising:

means for sending a registration request to the Home Agent;

means for receiving a registration reply from the Home Agent, the registration reply indicating that the Mobile Node is to derive a key to be shared between the Mobile Node and the Home Agent; and

means for deriving a key to be shared between the Mobile Node and the Home Agent from key information stored at the Mobile Node.